Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) An equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, wherein;

(1) said user-end equipment provided with individual user-end equipment information issued by said key center and individual user-end equipment secret information corresponding to said individual user-end equipment's information, and said user-end equipment transmits said individual user-end equipment information to said system-end equipment;

(2) said system-end equipment receives said individual user-end equipment information from said user-end equipment, reproduces by a system conversion said individual user-end equipment secret information from said received individual user-end equipment information using an equivalent secret key cryptographic algorithm of the key center, and authenticates said user-end equipment by confirming that said user-end equipment legitimately has said individual user-end equipment secret information by using a challenge response utilizing a common key cryptographic algorithm; and

(3) said user-end equipment and said system-end equipment execute a cryptographic communication with each other using said individual user-end equipment secret information.

2. (Original) The equipment authentication and cryptographic communication system according to claim 1, wherein:

(1) said system-end equipment is provided with system-end equipment secret information, which is identical to that possessed by said key center, and produces individual user-end equipment secret information from said individual user-end equipment information using said system-end equipment secret information; and

(2) said user-end equipment authenticates said system-end equipment by confirming that said system-end equipment has said individual user-end equipment secret information by a challenge response utilizing said common key cryptographic algorithm.

3. (Original) The equipment authentication and cryptographic communication system according to claim 1, wherein said system-end equipment is provided with a secret-key cryptographic algorithm, and reproduces said individual user-end equipment secret information by a system conversion of said individual user-end equipment information using a secret key.

4. (Original) The equipment authentication and cryptographic communication system according to claim 3, wherein said system-end equipment and said user-end equipment are both provided with common secret information shared therebetween by exchanging individually held secret information.

5. (Original) The equipment authentication and cryptographic communication system according to claim 4, wherein said system-end equipment and said user-end equipment (a) exchange with each other individually held secret information, and (b) generate new secret information by combining said individually held secret information and said secret information exchanged therebetween according to a predetermined procedure.

6. (Original) The equipment authentication and cryptographic communication system according to claim 5, wherein said system-end equipment and said user-end equipment use said individual user-end equipment secret information for encrypting said new secret information, which is provided by combining said information and said exchanged information.

7. (Original) The equipment authentication and cryptographic communication system according to claim 6, wherein said system-end equipment and said user-end equipment (a) individually generate random digits, (b) exchange said generated random digits with each

other, and (c) share the same secret information particular to said system-end equipment and said user-end equipment by combining said generated random digits and said exchanged random digits according to a predetermined procedure.

8. (Original) The equipment authentication and cryptographic communication system according to claim 7, wherein said system-end equipment and said user-end equipment (a) individually generate random digits, (b) combine said random digits with their own information particular to each of said system-end equipment and said user-end equipment according to a predetermined procedure, (c) generate encrypted data by encrypting the combined information using said individual user-end equipment secret information, (d) exchange said encrypted data with each other, (e) generate decrypted data by decrypting said exchanged encrypted data using said individual user-end equipment's secret information, and (f) reproduce each of said mutually exchanged random digits by dividing the combination of said decrypted data according to a predetermined procedure.

9. (Original) The equipment authentication and cryptographic communication system according to claim 8, wherein said system-end equipment and said user-end equipment (a) individually generate and store random digits, (b) exchange said random digits with each other, (c) combine said exchanged random digits with said individually generated and stored random digits according to a predetermined procedure, (d) generate encrypted data by encrypting said combined information using said individual user-end equipment secret information, (e) exchange said encrypted data with each other, (f) generate decrypted data by decrypting said exchanged encrypted data using said individual user-end equipment secret information, and (g) reproduce each of said mutually exchanged random digits by dividing the combination of said decrypted data according to a predetermined procedure.

10. (Original) The equipment authentication and cryptographic communication system according to claim 9, wherein said system-end equipment and said user-end equipment individually execute matching determinations by comparing said mutually exchanged random digits, which are produced by dividing the combination of said decrypted data according to the predetermined procedure, with said individually generated and stored random digits.

11. (Original) The equipment authentication and cryptographic communication system according to claim 10, wherein said system-end equipment and said user-end equipment produce and store the same data by combining said exchanged and received random digits and said individually generated and stored random digits according to the predetermined procedure, and mutually share said data as a common key particular to both said system-end equipment and said user-end equipment, if said matching determination produces a positive result.

12. (Currently Amended) An equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, wherein;

(1) said key center is provided with a first system converter for generating user-end equipment secret information from user-end equipment information;

(2) said user-end equipment is provided with a first storage unit for storing said user-end equipment information provided by said key center, a second storage unit for storing said user-end equipment secret information, a first encryption unit, and a first decryption unit; and

(3) said system-end equipment is provided with a second system converter for generating said user-end equipment secret information by a system conversion of said user-end equipment information received from said user-end equipment, a second encryption unit, and a second decryption unit, said second system converter using an equivalent secret key cryptographic algorithm of the first system converter to generate said user-end equipment secret information from said received user-end equipment information, and

wherein said user-end equipment and said system-end equipment share and utilize said user-end equipment secret information as a common key for encryption and decryption in said first encryption unit and said first decryption unit in said user-end equipment, and said second encryption unit and said second decryption unit in said system-end equipment.

13. (Original) The equipment authentication and cryptographic communication system according to claim 12, wherein:

(1) said user-end equipment further comprises a first random digit generator for generating a random digit, a second random digit generator for generating a random digit, a first combiner for combining a pair of random digit data according to a predetermined procedure, a first divider for dividing a combined pair of random digit data to reproduce original random digits prior to combining, a first common key generator for combining a pair of random digit data according to a predetermined procedure, and a first matching determination unit for determining if two random digit data match each other; and

(2) said system-end equipment further comprises a third random digit generator for generating a random digit, a fourth random digit generator for generating another random digit, a second combiner for combining a pair of random digit data according to a predetermined procedure, a second divider for dividing a combined pair of random digit data to reproduce original random digits prior to combining, a second common key generator for combining a pair of random digit data according to a predetermined procedure, and a second matching determination unit for determining if two random digit data match each other.

14. (Currently Amended) A method of equipment authentication and cryptographic communication for an equipment authentication and cryptographic communication system including user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, said method comprising the steps of:

(1) generating user-end equipment secret information from user-end equipment information in said key center;

(2) receiving said user-end equipment information and said user-end equipment secret information in said user-end equipment from said key center;

(3) receiving said user-end equipment information from said user-end equipment, and generating said user-end equipment secret information from said user-end equipment

information received in said system-end equipment by a system conversion using an equivalent secret key cryptographic algorithm of said key center; and

(4) using said user-end equipment secret information as a common key for encryption and decryption in both of said user-end equipment and said system-end equipment.

15. (Original) The method of equipment authentication and cryptographic communication according to claim 14 further comprising the steps of:

(1) generating a first random digit in said user-end equipment, and transmitting said first random digit to said system-end equipment;

(2) generating a second random digit in said system-end equipment, combining said second random digit and said first random digit received from said user-end equipment, encrypting combined data of said second random digit and said first random digit using said common key, and transmitting said encrypted data to said user-end equipment;

(3) decrypting said encrypted data received in said user-end equipment using said common key, and reproducing said first random digit and said second random digit by dividing decrypted data of said encrypted data received in said user-end equipment;

(4) determining in said user-end equipment if said first random digit reproduced in the preceding decryption step matches with another first random digit generated therein;

(5) generating a third random digit in said user-end equipment, combining said third random digit and said second random digit reproduced in the decryption step, encrypting combined data of said third random digit and said second random digit using said common key, and transmitting encrypted data of said combined data to said system-end equipment;

(6) generating a fourth random digit in said system-end equipment, and transmitting said fourth random digit to said user-end equipment;

(7) combining said fourth random digit received in said user-end equipment from said system-end equipment and said third random digit generated therein, encrypting combined data of said fourth random digit and said third random digit using said common key, and transmitting encrypted data of said combine data to said system-end equipment;

(8) decrypting said encrypted data received in said system-end equipment using said common key, and reproducing said third random digit and said fourth random digit by dividing decrypted data of said encrypted data received in said system-end equipment; and

(9) determining in said system-end equipment if said fourth random digit reproduced in the preceding decryption step matches with another fourth random digit generated therein.

16. (Original) The method of equipment authentication and cryptographic communication according to claim 15 further comprising the steps of:

producing data in said system-end equipment for use as a common key for cryptographic communication by combining said second random digit generated therein with said third random digit reproduced by decryption; and

producing data in said user-end equipment for use as a common key for cryptographic communication by combining said third random digit generated therein and said second random digit reproduced by decryption.

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (Cancelled)

27. (Cancelled)

28. (Cancelled)